



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/670,424	09/26/2000	Makoto Sato	00681/LH	5505

1933 7590 09/23/2005

FRISHAUF, HOLTZ, GOODMAN & CHICK, PC
220 5TH AVE FL 16
NEW YORK, NY 10001-7708

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT PAPER NUMBER

2136

DATE MAILED: 09/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/670,424

Applicant(s)

SATO ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 July 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 30-42 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 30-42 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

21

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

2. Applicant's submission filed on July 05, 2005 has been entered and made of record.

Response to Arguments

3. Applicant's arguments filed July 05, 2005 have been fully considered but they are not persuasive.

Specification

4. The amendment filed on July 05, 2005 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no

amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:

Examiner points to Page 26 lines 5 – 21 of the original specification filed on 9/26/2000 for disclosure on “Inputting retrieval information refers to inputting a column item to be retrieved, and a retrieving character string (keyword)” and “..it is determined whether or not the column item input to be retrieved is a pre-retrieval process column item. If ...for the column item”. The newly proposed amendment to the specification recites “that is, an item category title referring to a category of item to be retrieved), which shall introduce new matter as it broadens the scope of the invention. Original specification disclosed “a column item” to be used in a retrieving process and the data of that column item is encrypted using a common column key (see page 18 line 7 – Page 20 line 18). By introducing “.. an item category title referring to a category of item to be retrieved”, data that is retrieved in not bind to that particular column item.

Examiner reminds the applicant that the amendment to specification filled on June 03, 2005 has not been entered (please refer to Advisory action mailed on June 21, 2005) and Examiner respectfully requests that cancelled new matter or corrected amendment to the specification should reflect all the changes with respect to the original specification filled on 9/26/2000.

Examiner also suggests amending the specification as ““Inputting retrieval information refers to inputting a column item to be retrieved, and a retrieving character string (keyword) that is an item category title referring to a category of Column item to be retrieved” (emphasis added).

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 30 – 42 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended independent Claims 30, 33, 34, 37 and 39 – 42 recite, “...item category titles that identify respective categories of the data segment.”.

With respect to “respective categories”, the specification does not indicate how the item category title is used for example, with respect to “item category titles that

Art Unit: 2136

identify respective categories of the data segment". Applicant amendment does not clarify and Applicant remarks/arguments do not address "item category titles that identify respective categories of the data segment".

The dependent claims 31, 32, 35, 36 and 38 are rejected at least by virtue of their dependency on the dependent claims.

Regarding claims 30 – 42, Applicant argues that the CPA do not teach "whereby all of the database data segments in the data segment group(s) that are the target of the search are encrypted using a same column key, and whereby the (column) item category titles identify respective categories of the data segments". This argument is not found persuasive.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "whereby all of the database data segments in the data segment group(s) that are the target of the search are encrypted using a same column key, and whereby the (column) item category titles identify respective categories of the data segments") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Examiner directs to the claims 30, 33, 34, 37 and 39 – 42 which recite, "... an encryption unit ...the data segment of said at least one specified data segment group

Art Unit: 2136

that is the target of the data search process using the column key, and ... segments of at least one data segment group corresponding to item category titles other than the stored ... identify respective ..."). Prior art is believed to read on the claims as not all of the database data segments are encrypted but at least one data segment group is encrypted.

Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein an encryption unit for encrypting the data segments of at least one data segment group corresponding to item titles other than the stored item titles, in units corresponding to the records, using the different row keys of the respective records (Taguchi Column 3 line 64 – Column 4 line 15; Column 7 lines 40 – 65 and Column 11 lines 3 – 45).

Taguchi when combined with Goldstein, discloses encrypting the data segment using the different row keys of the respective records where encrypting the data segment using a column key to provide a database with internal-level data encryption and the encryption keys to depend on the attributes of the row and column keys.

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter "... an encryption unit ..the data segment of said at least one specified data segment group that is the target of the data search process using the column key, and ... segments of at least one data segment group corresponding to item category titles other than the stored ... identify respective ...")

Art Unit: 2136

broadly recited in the amended independent claims 30, 33, 34, 37 and 39 – 42. The dependent claims 31, 32, 35, 36 and 38 are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action.

Accordingly, the rejection for the pending claims 30 – 42 is respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 30 –42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldstein (U.S. Patent Number 5,963,642, hereafter “Goldstein”) in view of Taguchi et al. (U.S. Patent Number 5,915,025 hereafter “Taguchi”).

7. Regarding Claim 30, Goldstein teaches and describes

a database storage unit which stores a database comprising a plurality of records each record including a plurality of data segments identified by item category titles that identify respective categories of the data segments(Goldstein Fig. 5, 6A&B; Column 10 lines 28 – 50 and Column 12 lines 38 – 58);

an item title storing unit for storing at least one item category title for specifying a corresponding at least one data segment group as a target of a data search process (Goldstein Column 12 line 64 – Column 13 line 3);

a key data storing unit for storing keys for use in encryption associated with the database, wherein the keys comprise a column key corresponding to the at least one data segment group specified by the at least one stored item category title, and a plurality of different row keys corresponding respectively to the records of the database (Goldstein Column 11 line 63 – Column 12 line 9 and Column 14 line 53 – Column 15 line 14); and

an encryption unit for encrypting: (i) the data segments of said at least one specified data segment group using the corresponding column key, and (ii) data segments of at least one data segment group corresponding to item category titles other than the stored item category titles, in units corresponding to the records, using the different row keys of the respective records (Goldstein Column 25 line 36 – Column 26 line 22).

8. Even though Goldstein discloses encrypting the data segment using a column key, Goldstein does not explicitly disclose encrypting the data segment group corresponding to item titles other than the stored item category titles, in units corresponding to the records, using the different row keys of the respective records. However, Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein an encryption

unit for encrypting the data segments of at least one data segment group corresponding to item category titles other than the stored item category titles, in units corresponding to the records, using the different row keys of the respective records (Taguchi Column 3 line 64 – Column 4 line 15; Column 7 lines 40 – 65 and Column 11 lines 3 – 45).

9. Motivation to combine the invention of Goldstein and Taguchi comes from the need for encrypting data by using the column and row keys in a database to provide internal-level encrypted data for faster retrieval and for database information to be locally decrypted. Goldstein provides a discussion for the need for plurality of column keys to encrypt the data by using plurality of column permutations but silent on using plurality of row permutations (Goldstein Column 17 line 53 – Column 18 line 31 and Column 24 and line 34 – column 26 line 29; especially Column 26 lines 5 – 22). It would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Taguchi which discloses encrypting the data segment using the different row keys of the respective records with the teachings of Goldstein where encrypting the data segment using a column key to provide a database with internal-level data encryption and the encryption keys to depend on the attributes of the row and column keys.

10. Regarding Claim 33, Goldstein teaches and describes

a functional unit which encrypts: data segments forming data segment groups corresponding to column item category titles of a first kind using a column key common

to the data segment groups and, data segments forming data segment groups corresponding to column item category titles of a second kind, in units of rows of data segments, using respective row keys, said item category titles identifying respective categories of the data segments (Goldstein Column 25 lines 36 – Column 26 line 22);

wherein the second information processor terminal comprises:

a transmitting unit which transfers via the network, an encrypted data set representing conditions to be used for the search process in the first information processor terminal, when the second information processor terminal requests the first information processor terminal to perform the search process on the database, said encrypted data set being formed by encrypting an input data set specifying the conditions of the search process by using the column key (Goldstein Fig. 6A&B, 10A&B; Column 14 lines 24 – 52 and Column 15 lines 22 – 31); and

wherein the first information processor terminal further comprises :

a search performing unit that performs the search process on the encrypted database, based on the transmitted encrypted data set; and a returning unit that returns an encrypted result data set resulting from the search process, to the second information processing terminal via the network (Goldstein Column 14 lines 24 – 52 and Column 15 lines 1 – 4).

11. Even though Goldstein discloses encrypting the data segment using a column key, Goldstein does not explicitly discloses encrypting the data segments forming data segment groups corresponding to column item titles of a second kind, in units of rows of

Art Unit: 2136

data segments, using respective row keys. However, Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein an encryption unit for encrypting the data segments of at least one data segment forming data segment groups corresponding to column item titles of a second kind, in units of rows of data segments, using respective row keys (Taguchi Column 3 line 64 – Column 4 line 15; Column 7 lines 40 – 65 and Column 11 lines 3 – 45).

12. Motivation to combine the invention of Goldstein and Taguchi comes from the need for encrypting data by using the column and row keys in a database to provide internal-level encrypted data for faster retrieval and for database information to be locally decrypted. Goldstein provides a discussion for the need for plurality of column keys to encrypt the data by using plurality of column permutations but silent on using plurality of row permutations (Goldstein Column 17 line 53 – Column 18 line 31 and Column 24 and line 34 – column 26 line 29; especially Column 26 lines 5 – 22). It would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Taguchi which discloses encrypting the data segment using the different row keys of the respective records with the teachings of Goldstein where encrypting the data segment using a column key to provide a database with internal-level data encryption using both permutations of column and row keys as the encryption keys to depend on the attributes of the row and column keys.

Art Unit: 2136

13. Regarding Claim 34, Goldstein teaches and describes a database management apparatus comprising:

a key specification storing unit that memorizes data specifying a type of encryption system to be used to encrypt data segments of each column of a database, if the column of the database is to be encrypted (Goldstein Column 11 line 63 – Column 12 line 9 and Column 14 line 53 – Column 15 line 14);

a first encryption unit that encrypts in accordance with the data stored by the key specification storing unit: (i) data segments forming data segment groups corresponding to column item category titles of a first kind using a same column key, and (ii) data segments forming data segment groups corresponding to column item category titles of a second kind, in units of rows of the database, using row keys respectively specified for each of the rows, said item category titles identifying respective categories of the data segments (Goldstein Column 25 line 36 – Column 26 line 22);

a second encryption unit that encrypts, using a basic key, all of the row keys used by the first encryption unit (Goldstein 22 lines 49 – 17), Goldstein discloses that the codebook entries (column keys) are encrypted using a public (basic) key cryptography;

a key data generating unit that generates the column key, the row keys and the basic key (Goldstein Column 23 lines 28 – 45 and 26 lines 22), Goldstein discloses that a trusted key server (generate and administer keys) can provide authorization to exchange keys; and

a storing operation unit which stores in a memory the database after encryption by the first encryption unit and the row keys after encryption by the second encryption unit, in a mutually associated manner (Goldstein Column 22 lines 55 – 61).

14. Even though Goldstein discloses encrypting the data segment using a column key, Goldstein does not explicitly disclose encrypting the data segments forming data segment groups corresponding to column item titles of a second kind, in units of rows of data segments, using respective row keys. However, Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein an encryption unit for encrypting the data segments of at least one data segment forming data segment groups corresponding to column item titles of a second kind, in units of rows of data segments, using respective row keys (Taguchi Column 3 line 64 – Column 4 line 15; Column 7 lines 40 – 65 and Column 11 lines 3 – 45).

15. Motivation to combine the invention of Goldstein and Taguchi comes from the need for encrypting data by using the column and row keys in a database to provide internal-level encrypted data for faster retrieval and for database information to be locally decrypted. Goldstein provides a discussion for the need for plurality of column keys to encrypt the data by using plurality of column permutations but silent on using plurality of row permutations (Goldstein Column 17 line 53 – Column 18 line 31 and Column 24 and line 34 – column 26 line 29; especially Column 26 lines 5 – 22). It would

Art Unit: 2136

be obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Taguchi which discloses encrypting the data segment using the different row keys of the respective records with the teachings of Goldstein where encrypting the data segment using a column key to provide a database with internal-level data encryption using both permutations of column and row keys as the encryption keys to depend on the attributes of the row and column keys.

16. Regarding Claim 37, Goldstein teaches and describes

encrypting the database by encrypting, on a first terminal side of the system:(i) data segments forming data segment groups corresponding to column item category titles of a first kind using a same column key, (ii) data segments forming data segment groups corresponding to column item category titles of a second kind, in units of rows of the database, using Low keys respectively specified for each of the rows, and (iii) all of the row keys, using another key, said item category titles identifying respective categories of the data segments (Goldstein Column 22 lines 49 – 17 and Column 25 line 36 – Column 26 line 22), Goldstein discloses that the data is encrypted using a public (another) key cryptography;

searching the encrypted database stored on any of the distributed storage medium units, decrypting a data set obtained as a search result and displaying the decrypted data set at a second terminal unit side of the system network (Goldstein Column 14 lines 24 – 52 and Column 15 lines 1 – 4).

17. Even though Goldstein discloses encrypting the data segment using a column key, Goldstein does not explicitly disclose encrypting the data segments forming data segment groups corresponding to column item titles of a second kind, in units of rows of data segments, using respective row keys. However, Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein an encryption unit for encrypting the data segments of at least one data segment forming data segment groups corresponding to column item titles of a second kind, in units of rows of data segments, using respective row keys (Taguchi Column 3 line 64 – Column 4 line 15; Column 7 lines 40 – 65 and Column 11 lines 3 – 45). Goldstein discloses storing the encrypted database on storage medium units for distribution (Goldstein Fig. 5, 6A&B; Column 10 lines 28 – 50 and Column 12 lines 38 – 58), Goldstein does not explicitly disclose such storage medium is a portable storage medium unit for distribution. However, Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein the encrypted database is stored on portable (CD) storage medium.

18. Motivation to combine the invention of Goldstein and Taguchi comes from the need for encrypting data by using the column and row keys in a database to provide internal-level encrypted data for faster retrieval and for database information to be locally decrypted. Goldstein provides a discussion for the need for plurality of column keys to encrypt the data by using plurality of column permutations but silent on using

Art Unit: 2136

plurality of row permutations (Goldstein Column 17 line 53 – Column 18 line 31 and Column 24 and line 34 – column 26 line 29; especially Column 26 lines 5 – 22). It would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Taguchi which discloses encrypting the data segment using the different row keys of the respective records and using a CD as a portable storage medium for easy distribution with the teachings of Goldstein where encrypting the data segment using a column key to provide a database with internal-level data encryption using both permutations of column and row keys as the encryption keys to depend on the attributes of the row and column keys.

19. Regarding Claim 39, Goldstein teaches and describes

encrypt, in a first mode, data segments forming data segment groups corresponding to column item category titles of a first kind using a same column key, said data segments forming the data segment groups, said data segments being elements of a database (Goldstein Column 22 lines 49 – 17 and Column 25 line 36 – Column 26 line 22),

encrypt, in a second mode, data segments forming data segment groups corresponding to column item category titles of a second kind using respective row keys corresponding to respective rows of the database (Goldstein Column 22 lines 49 – 17 and Column 25 line 36 – Column 26 line 22); and

encrypting all the row keys used in the second mode using another key assigned commonly for the respective rows wherein the item category titles identify respective categories of the data segments (Goldstein Column 22 lines 49 – 17 and Column 25 line 36 – Column 26 line 22), Goldstein discloses that the data is encrypted using a public (another) key cryptography.

20. Even though Goldstein discloses encrypting the data segment using a column key, Goldstein does not explicitly discloses encrypting in a second mode, data segments forming data segment groups corresponding to column item titles of a second kind using respective row keys corresponding to respective rows of the database. However, Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein an encryption unit for encrypting, in a second mode, data segments forming data segment groups corresponding to column item titles of a second kind using respective row keys corresponding to respective rows of the database (Taguchi Column 3 line 64 – Column 4 line 15; Column 7 lines 40 – 65 and Column 11 lines 3 – 45).

21. Motivation to combine the invention of Goldstein and Taguchi comes from the need for encrypting data by using the column and row keys in a database to provide internal-level encrypted data for faster retrieval and for database information to be locally decrypted. Goldstein provides a discussion for the need for plurality of column keys to encrypt the data by using plurality of column permutations but silent on using

Art Unit: 2136

plurality of row permutations (Goldstein Column 17 line 53 – Column 18 line 31 and Column 24 and line 34 – column 26 line 29; especially Column 26 lines 5 – 22). It would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Taguchi which discloses encrypting the data segment using the different row keys of the respective records with the teachings of Goldstein where encrypting the data segment using a column key to provide a database with internal-level data encryption using both permutations of column and row keys as the encryption keys to depend on the attributes of the row and column keys.

22. Regarding Claim 40, Goldstein teaches and describes a database management apparatus comprising:

a database storage unit which stores a database comprising a plurality of records each record including a plurality of data segments identified by item category titles that identify respective categories of the data segments (Goldstein Fig. 5, 6A&B; Column 10 lines 28 – 50 and Column 12 lines 38 – 58);

an item category title storing unit. for storing at least one item title for specifying a corresponding at least one data segment group as a target of a data search process (Goldstein Column 12 line 64 – Column 13 line 3);

a key data storing unit for storing keys for use in encryption associated with the database, wherein the keys comprise a column key corresponding to the at least one data segment group specified by the at least one stored item title, and a plurality of

Art Unit: 2136

different row keys corresponding respectively to the records of the database (Goldstein Column 11 line 63 – Column 12 line 9 and Column 14 line 53 – Column 15 line 14); and

an encryption unit for encrypting: (i) the data segments of said at least one specified data segment group that is the target of the data search process using the column key corresponding to the at least one specified data segment group, and (ii) data segments of at least one data segment group corresponding to item category titles other than the at least one stored item category titles, in units corresponding to the records, using the different row keys of the respective records and another column key that is assigned commonly to the data segment groups corresponding to item category titles other than the at least one stored item category title (Goldstein Column 25 line 36 – Column 26 line 22).

23. Even though Goldstein discloses encrypting the data segment using a column key, Goldstein does not explicitly disclose encrypting the data segment group corresponding to item titles other than the stored item titles, in units corresponding to the records, using the different row keys of the respective records. However, Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein an encryption unit for encrypting the data segments of at least one data segment group corresponding to item titles other than the stored item titles, in units corresponding to the records, using the different row keys of the respective records (Taguchi Column 3 line 64 – Column 4 line 15; Column 7 lines 40 – 65 and Column 11 lines 3 – 45).

23. Motivation to combine the invention of Goldstein and Taguchi comes from the need for encrypting data by using the column and row keys in a database to provide internal-level encrypted data for faster retrieval and for database information to be locally decrypted. Goldstein provides a discussion for the need for plurality of column keys to encrypt the data by using plurality of column permutations but silent on using plurality of row permutations (Goldstein Column 17 line 53 – Column 18 line 31 and Column 24 and line 34 – column 26 line 29; especially Column 26 lines 5 – 22). It would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Taguchi which discloses encrypting the data segment using the different row keys of the respective records with the teachings of Goldstein where encrypting the data segment using a column key to provide a database with internal-level data encryption and the encryption keys to depend on the attributes of the row and column keys.

24. Regarding Claim 41, Goldstein teaches and describes a computer program for directing a computer to execute functions comprising:

accessing a database comprising a plurality of records, each record including a plurality of data segments identified by item category titles that identify respective categories of the data segments (Goldstein Fig. 5, 6A&B; Column 10 lines 28 – 50 and Column 12 lines 38 – 58);

storing at least one item category title for specifying a corresponding at least one data segment group as a target of a data search process (Goldstein Column 12 line 64 – Column 13 line 3);

storing keys or use in encryption associated with the database, wherein the keys comprise a column key corresponding to said at least one data segment group specified by the at least one stored item category title, and a plurality of different row keys corresponding respectively to the records of the database (Goldstein Column 12 line 64 – Column 13 line 3; Column 11 line 63 – Column 12 line 9 and Column 14 line 53 – Column 15 line 14);

encrypting: (i) the data segments of said at least one specified data segment group that is the target of the data search process using the column key corresponding to the at least one specified data segment group, and (ii) data segments of at least one data segment group corresponding to item category titles other than the at least the stored item category titles, in units corresponding to the records, using the different row keys of the respective records (Goldstein Column 25 line 36 – Column 26 line 22).

25. Even though Goldstein discloses encrypting the data segment using a column key, Goldstein does not explicitly discloses encrypting the data segment group corresponding to item titles other than the stored item titles, in units corresponding to the records, using the different row keys of the respective records. However, Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein an encryption unit for encrypting the

data segments of at least one data segment group corresponding to item titles other than the stored item titles, in units corresponding to the records, using the different row keys of the respective records (Taguchi Column 3 line 64 – Column 4 line 15; Column 7 lines 40 – 65 and Column 11 lines 3 – 45).

26. Motivation to combine the invention of Goldstein and Taguchi comes from the need for encrypting data by using the column and row keys in a database to provide internal-level encrypted data for faster retrieval and for database information to be locally decrypted. Goldstein provides a discussion for the need for plurality of column keys to encrypt the data by using plurality of column permutations but silent on using plurality of row permutations (Goldstein Column 17 line 53 – Column 18 line 31 and Column 24 and line 34 – column 26 line 29; especially Column 26 lines 5 – 22). It would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Taguchi which discloses encrypting the data segment using the different row keys of the respective records with the teachings of Goldstein where encrypting the data segment using a column key to provide a database with internal-level data encryption and the encryption keys to depend on the attributes of the row and column keys.

27. Regarding Claim 42, Goldstein teaches and describes a computer program for directing a computer to execute functions comprising:

storing data specifying a type of encryption system to be used to encrypt data segments of each column of a database, if the column of the database is to be encrypted (Goldstein Column 12 line 64 – Column 13 line 3)

first encrypting in accordance with the data stored by the key specification memory: (i) data segments forming data segment groups corresponding to column item category titles of a first kind using a same column key for said data segments forming the segment groups, and (ii) data segments forming data segment groups corresponding to column item titles of a first kind using a same column key, and data segments forming data segment groups corresponding to column item titles of a second kind, in units of rows of the database, using row keys respectively specified for each of the rows, said item category titles identifying respective categories of the data segments (Goldstein Column 25 line 36 – Column 26 line 22);

second encrypting, with a basic key, all the row keys (Goldstein 22 lines 49 – 17), Goldstein discloses that the codebook entries (column keys) are encrypted using a public (basic) key cryptography; and

storing in a memory the database after the encryption thereof and the row keys after encryption the encryption thereof, in a mutually associated manner (Goldstein Column 22 lines 55 – 61).

28. Even though Goldstein discloses encrypting the data segment using a column key, Goldstein does not explicitly discloses encrypting the data segment group corresponding to item titles other than the stored item titles, in units corresponding to

the records, using the different row keys of the respective records. However, Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein an encryption unit for encrypting the data segments of at least one data segment group corresponding to item titles other than the stored item titles, in units corresponding to the records, using the different row keys of the respective records (Taguchi Column 3 line 64 – Column 4 line 15; Column 7 lines 40 – 65 and Column 11 lines 3 – 45).

29. Motivation to combine the invention of Goldstein and Taguchi comes from the need for encrypting data by using the column and row keys in a database to provide internal-level encrypted data for faster retrieval and for database information to be locally decrypted. Goldstein provides a discussion for the need for plurality of column keys to encrypt the data by using plurality of column permutations but silent on using plurality of row permutations (Goldstein Column 17 line 53 – Column 18 line 31 and Column 24 and line 34 – column 26 line 29; especially Column 26 lines 5 – 22). It would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Taguchi which discloses encrypting the data segment using the different row keys of the respective records with the teachings of Goldstein where encrypting the data segment using a column key to provide a database with internal-level data encryption and the encryption keys to depend on the attributes of the row and column keys.

Art Unit: 2136

30. Claim 31 is rejected applied as above in rejecting Claim 30. Furthermore, Goldstein teaches and describes a database management apparatus further comprising:

a functional unit which encrypts a received data set comprising a search process condition using the corresponding column key (Goldstein Fig. 5, 6A&B; Column 10 lines 28 – 50 and Column 12 line 64 – Column 13 line 3); and

database search unit which performs the data search process by comparing the encrypted search process condition with the encrypted data segments of said at least one specified group.(Goldstein Column 14 line 53 – Column 15 line 4).

31. Claim 32 is rejected applied as above in rejecting Claim 30. Furthermore, Goldstein teaches and describes a database management apparatus, wherein the encryption unit sequentially generates vectors in a multidimensional space based on a set of predetermined functions, and the data segments are encrypted in accordance with an encryption method in which components of the sequentially generated vectors form a key stream of a key associated with the encryption method (Goldstein Column 7 line 48 – Column 8 line 67 and Column 25 lines 5 – 59), and

wherein the row keys and the column key specify constants of the functions (Goldstein Column 8 lines 60 – 66).

32. Claim 35 is rejected applied as above in rejecting Claim 34. Furthermore, Goldstein teaches and describes a database management apparatus, wherein the

row keys are each generated based on a number of the respective rows and a random number (Goldstein Column 22 lines 12 – 17 and Column 26 line 22).

33. Even though Goldstein discloses generating column key based on a column number and a random number, Goldstein does not explicitly disclose row keys are generated based on a number of the respective rows and a random number. However, Taguchi discloses a data processing apparatus with software protecting functions capable of enhancing the level of encryption security wherein row keys are generated based on a number of the respective rows and a random number (Taguchi Column 14 lines 1 – 19).

34. Motivation to combine the invention of Goldstein and Taguchi comes from the need for encrypting data by using the column and row keys in a database to provide internal-level encrypted data for faster retrieval and for database information to be locally decrypted. Goldstein provides a discussion for the need for plurality of column keys to encrypt the data by using plurality of column permutations but silent on using plurality of row permutations (Goldstein Column 17 line 53 – Column 18 line 31 and Column 24 and line 34 – column 26 line 29; especially Column 26 lines 5 – 22). It would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Taguchi which discloses generating a key with a random number and using the different row keys of the respective records with the teachings of Goldstein where encrypting the data segment using a column key to provide a database

Art Unit: 2136

with internal-level data encryption and the encryption keys to depend on the attributes of the row and column keys.

35. Claim 36 is rejected applied as above in rejecting Claim 34. Furthermore, Goldstein teaches and describes a database management apparatus, wherein a vector generation unit sequentially generates vectors confined to a closed subspace of an n-dimensional space and defined by functions based on the keys (Goldstein Column 7 line 48 – Column 8 line 67 and Column 25 lines 5 – 59); and

wherein a logical operation unit performs a logical operation in units of a bit involving both the data segments of the database and components of the vectors generated by the vector generation unit, to encrypt the data segments (Goldstein Column 8 lines 60 – 66).

36. Claim 38 is rejected applied as above in rejecting Claim 34. Furthermore, Goldstein teaches and describes a method for managing a database system including a first terminal unit for managing the database and a second terminal unit for searching the database independently of the first terminal unit (Goldstein Fig. 5, 6A&B; Column 10 lines 28 – 50 and Column 12 line 64 – Column 13 line 3), wherein each of the storage medium unit stores both the encrypted database generated by the first terminal unit, and a predetermined application program for performing a searching process on the encrypted database .(Goldstein Column 14 line 53 – Column 15 line 4).

Conclusion

37. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

38. Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to

Art Unit: 2136

the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy

September 13, 2005.


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100